

俄罗斯跨境数据流动立法规则与执法实践

何波

中国信息通信研究院互联网法律研究中心, 北京 100191

摘要

伴随着全球数字经济的迅猛发展,跨境数据流动监管越来越成为各方关注的焦点,俄罗斯出于安全考虑成为对跨境数据流动严格限制的代表国家。从俄罗斯数据管理法律框架出发,重点梳理了其跨境数据流动管理规则的立法变迁,分析了强力推行数据本地存储的原因,并考察了该规则的实施效果和监管机构的执法检查情况。最后,提出了对中国跨境数据流动管理的启示和建议。

关键词

跨境数据流动;本地化存储;数据立法;监督检查

中图分类号:D95

文献标识码:A

doi: 10.11959/j.issn.2096-0271.2016073

Legislation and enforcement of cross-border data flows rules in Russia

HE Bo

Internet Law Center of China Academy of Information and Communication Technology, Beijing 100191, China

Abstract

With the rapid development of global digital economy, the cross-border data flows are becoming an important issue of concern. For the sake of data security, Russia has imposed a strict limitation on cross-border data flows. The legislation system of Russian's data regulation and the establishment of cross-border data flows rules were discussed in detail and the reasons of local retention requirement in Russia were analyzed either. In the end, several suggestions were given.

Key words

cross-border data flow, local retention, data legislation, supervision and inspection

1 引言

对跨境数据流动进行管理是一国行使其数据主权的重要体现,是否要求在一国境内存储和处理用户数据则是近年来各国立法的主要分歧所在。当前,随着全球数字经济的发展,美国不断致力于倡导和推动数据全球自由流动,例如,在美国主导的《跨太平洋伙伴关系协定》中明确指出:当通过电子方式跨境传输信息是为涵盖的人执行其业务时,缔约方应允许此跨境传输,包括个人信息,但以俄罗斯、欧盟为代表的国家和地区采取了与美国截然不同的做法。欧盟从个人数据保护角度出发,不断强化对数据跨境流动的管理,2016年4月新通过的《一般数据保护条例》再次严格限定了数据向欧盟成员国境外跨境流动的条件。俄罗斯在2013年“棱镜计划”曝光以后,基于维护国家安全的历史传统和现实中的网络数据安全威胁,通过两次修改立法,明确提出公民数据的存储和处理必须在俄罗斯境内进行,成为强行实施数据本地化存储的典型代表。

然而,俄罗斯跨境数据流动管理法律体系是如何形成的以及本地化留存要求的具体内容到底是什么,目前并没有一个准确、系统的研究和梳理,对于俄罗斯数据本地化生效后的实施效果和执法监管也缺乏有效的介绍。本文从俄罗斯数据管理法律框架出发,重点梳理了俄罗斯跨境数据流动管理规则的立法变迁和具体内容,分析了俄罗斯强力推行数据本地存储的原因,并考察了该规则的实施效果和监管机构的执法检查情况,最后提出了我国跨境数据流动管理的建议。

2 俄罗斯数据管理的法律框架与本地化规则的确立

2.1 良好的数据管理立法基础

早在10年前,俄罗斯就建立起较为完善的信息保护和数据管理等法律制度。从立法体系看,其目前涉及数据管理的国家专门立法有两部,即《关于信息、信息技术和信息保护法》(第149号法令)^①和《俄罗斯联邦个人数据法》(第152号法令)^②。此外,《俄罗斯联邦大众传媒法》《俄罗斯联邦安全局法》《俄罗斯联邦外国投资法》等法律也对数据管理做出了相关规定和要求。

《关于信息、信息技术和信息保护法》于2006年由俄罗斯联邦议会通过,用以取代包括1995年《关于信息、信息化和信息保护法》在内的多部联邦法律。该法主要调整相关主体在进行寻找、获得、传递、生产和传播信息以及使用信息技术和进行信息保护时产生的法律关系。法令规定了信息所有者、信息系统运营者需要承担的信息保护义务,包括:预防非法获取信息和(或)将其传递给无权获取该信息的人员;及时发现非法获取信息的事实;对违法获取信息规定可能产生的后果进行警告;不采取破坏信息处理设备和手段功能的行为;迅速恢复因非法获取信息而被异化和销毁的信息;经常检查信息保护水平。

《俄罗斯联邦个人数据法》同样确立于2006年,该法旨在保障公民个人数据处理中的权利和自由,并对个人数据的跨境转交提出了同等保护的要求。该法规定:在进行个人数据跨境转交前,处理者有义务确认数据跨境转交的其他国家保证会对个人数据主体的权利进行同等保护;拥有同等保护的其他国家实施的个人数据跨境转交依照本法

①

http://www.wipo.int/wipolex/en/text.jsp?file_id=371639

②

https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf

进行；为了保护俄罗斯联邦宪法制度体系，维护道德、保护公民权利以及保障国防和国家安全，可以中止或者限制数据跨境转交行为。该法同时提出了同等保护的例外情况。

2.2 确立数据本地化基本规则

“棱镜门”事件后，俄罗斯开始启动修法进程，加强对跨境数据流动的管理，并相继发布了两个法令，确立其数据本地化存储的规则。

2014年5月7日，俄罗斯发布联邦第97号法令《俄罗斯联邦〈关于信息、信息技术和信息保护法〉修正案及个别互联网信息交流规范的修正案》对《关于信息、信息技术和信息保护法》进行了修改。在“互联网信息传播组织者的义务”中增加了境内留存的要求，规定：自网民接收、传递、发送和（或）处理语音信息、书面文字、图像、声音或者其他电子信息6个月内，互联网信息传播组织者必须在俄罗斯境内对上述信息及网民个人信息进行保存。同时，修正案还要求互联网信息传播组织者有义务保留和（或）提供给国家侦查机关和安全机关上述信息，不履行者将进行行政罚款。根据规定，该修正案自2014年8月1日起正式生效施行。

同年7月，总统普京签署联邦第242号法令《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》，对两部数据管理法律同时做了修改。在《关于信息、信息技术和信息保护法》第十六条第四款中增加一项，要求信息所有者、信息系统运营方有义务对俄罗斯联邦公民个人信息进行收集、记录、整理、保存、核对（更新、变动）、提取的数据库存放在俄罗斯境内。在《俄罗斯联邦个人数据法》第十八条增加第五款，要求收集个人数据（包括使用互联网手段）时，运营商需要保证使用位于俄罗斯境内的数据库，对

俄罗斯公民的个人数据进行搜集、记录、整理、保存、核对（更新、变动）和提取。此外，本条还要求数据处理者在处理数据前，要告知数据保护机关包含俄罗斯公民个人数据的数据库所在地的信息，并且根据俄罗斯联邦法律规定，对违反俄罗斯联邦个人数据法的信息进行限制访问。

通过两次修法，俄罗斯以立法的形式规定了互联网信息服务组织传播者、信息所有者以及运营商等主体的义务，同时也确立了数据本地存储的基本规则，主要包括3个方面：一是公民个人信息及相关信息和数据库需要在俄罗斯境内存储；二是对俄罗斯公民的个人数据的处理活动需要使用俄罗斯境内的数据库，即处理活动需要在俄境内进行；三是相关信息告知和协助有关部门执法的义务。总结来看，俄罗斯的立法规定十分严格，通过对企业施加法定的义务实现了政府对数据存储、跨境传输、处理等环节的全面控制，从而掌握了本国数据跨境流动的主动权。

3 推行数据本地存储的深层原因

俄罗斯对跨境数据流动管理的态度经历了由放任到确保网络安全的转变。在前一届政府任期内，时任总统梅德韦杰夫和总理普京在谈到国家对网络进行监管的问题时，都曾公开表态称，俄罗斯政府不会直接介入互联网的管理。然而“棱镜门”事件后，俄罗斯对跨境数据流动管理的态度发生了重大转变。导致这一变化的原因，除了国外监控的威胁外，还与俄罗斯的历史传统和数据安全现状有关。

3.1 直接原因

“棱镜门”事件是推动俄罗斯数据本地

化立法的直接原因。2013年,斯诺登揭露了美国全球监控计划,出于对本国安全的担忧,俄罗斯开始考虑加强网络监控和强化数据跨境流动管理。俄罗斯信息政策和信息技术及通信委员会的一名发言人呼吁俄罗斯应该加强其“数据主权”,通过立法要求电子邮件、社交网站等企业将其收集的俄罗斯用户的数据在俄境内留存^③。2013年春,俄罗斯通信部起草了一份法令草案,要求电信和互联网提供者在提供服务时安装可以收集和留存数据的设备^④,这被认为是数据本地化要求的前兆。

③

http://rbth.ru/politics/2013/06/21/lawmakers_seek_to_bolster_russias_internet_sovereignty_27365.html

④

<http://www.gpd-digital.org/gpd-update/data-collectionand-retention-in-russia/>

⑤

<http://www.cww.net.cn/news/html/2013/1/1/201311113844871.htm>

⑥

<http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/russia-changes-effective-date-of-data-localization-law-to-september-2015/>

⑦

<http://tech.qq.com/a/20150912/008162.htm>

3.2 历史原因

长期以来对国家安全的关注是俄罗斯实施数据本地化的历史原因。一直以来俄罗斯都重点关注国防、军事等传统安全领域。近几年,网络空间逐渐被视为继陆、海、空、天之后的“第五空间”,成为大国博弈的关注焦点和热点,网络主权和数据主权概念相继被突出。数据对政治、经济、文化、军事、外交的影响日益深刻和广泛,作为一种新的战略资源,是各国竭力拓展和争夺的新疆域,并已成为影响国际关系的重要因素。数据安全问题已成为国家安全的重要组成部分,俄罗斯作为国家安全意识极强的一个国家,非常注重数据安全的问题。

3.3 现实需求

网络攻击和数据泄露是俄罗斯建立数据本地留存制度的现实需求。从数据看,俄罗斯国内虽尚未发生危及国家安全的重大网络攻击事件,但长期面临大量网络攻击,潜在隐患不少。根据俄联邦安全局的统计数据,俄罗斯总统办公厅、国家杜马、联邦委员会网站每天遭受黑客攻击达1万余次。根据通信世界网的报道,俄罗斯数次成为全

球网络安全风险最高的国家^⑤。为了提高网络安全和数据安全的应对和管理,俄罗斯适时推出了数据留存本地化的管理要求。

4 数据本地存储规则的实施效果

如前所述,第242号法令最终确立了俄罗斯数据本地化留存的制度,要求俄罗斯公民个人数据必须存储在俄联邦境内的服务器上,该法令也被称为“数据本地化法”。“数据本地化法”原定于2016年9月1日生效,但2014年12月,俄罗斯总统普京签署526-FZ号联邦法令,将生效日期提前至2015年9月1日^⑥。第242号法令不能追溯既往,不适用于2015年9月1日前收集的个人数据。至此,俄罗斯建立了相对严格的跨境数据流动制度,并据此开展了相关的监督检查工作,配备专门工作人员负责调查相关企业公司是否遵守了这一规定。

4.1 各方态度

俄罗斯的数据本地化存储要求从酝酿到正式立法出台,其争论从来没有停止过,各方都站在自己立场展开争论,国外的互联网企业也出现了两种截然不同的态度。

以苹果、易趣为代表的企业本着务实的态度,主动落实俄罗斯数据存储“本土化”要求。在法案公布后,全球购物网站巨头易趣公司表示该公司愿意接受俄罗斯政府的指令,并宣布将把俄罗斯的用户数据转存至俄罗斯服务器。与此同时,据俄罗斯地方媒体报道,苹果公司和莫斯科市的互联网公司IXcellerate进行了合作,俄罗斯苹果公司用户的云服务数据将保存在对方的数据中心^⑦。以微软、谷歌为代表的数家公司都曾对俄罗斯数据本地化要求表示了反对,并威胁退出俄罗斯市场。在新规定

公布之后,谷歌宣布关闭在俄罗斯的工程技术部门,一共涉及100多名员工,但是广告销售、技术支持等部门仍继续留在俄罗斯;微软已经让其Skype开发团队撤离俄罗斯;而Adobe则完全退出了俄罗斯^⑧。

可以看出,数据存储本地化的要求给外国企业在俄罗斯开展业务带来了一定的障碍,需要在俄罗斯境内租用或建设新的数据库,给企业增加了更多的成本负担。中国互联网企业正在大幅进军俄罗斯市场,也需要按照俄方要求将俄罗斯公民的数据存储在对方境内。未来,俄罗斯数据本地化存储规制给我国企业带来的影响将逐步显现。

4.2 实施方式: 取于执法

数据存储本土化规则自2015年9月开始正式实施,随后俄罗斯监管机构Roskomnadzor对317家企业进行了检查,发现只有两家当地企业违反了数据本地化要求的规定。俄罗斯通信与大众传播部部长Nikolai Nikiforov表示,俄罗斯联邦政府的目的不是限制国外在线服务和资源,承诺不会利用检查企业来关闭外国网站^⑨。2016年1月,俄罗斯监管机构Roskomnadzor公布了2016年度详细的检查计划,以核查相关商业机构是否遵循要求,包括微软、三星、惠普、VKontakte(俄罗斯著名社交网站)、Ostrovok.Ru(俄罗斯酒店预订网站)、LaModa.ru(俄罗斯在线购物网站)等都在检查之列^⑩。截至2016年6月,根据Roskomnadzor负责人Mr. Zharov的介绍,在监管机构2016年进行的645次检查中,大多数企业都很好地遵守了数据本地留存的规定,仅发现了4家违规企业。监管机构进行了轻微罚款,并给予了其6个月的时间限期进行改正^⑪。

俄罗斯监管机构同时介绍,目前已经有

45 000家企业通知监管机构,其已经遵守了俄罗斯数据本地存储的要求,即将收集的俄公民个人数据留存在俄罗斯境内的数据库。按照计划,到2016年底,监管机构还计划对另外910家公司合规情况进行检查,使接受检查的公司总数超过1 500家。美国两家社交网站巨头Facebook和Twitter暂时不在2016年的检查计划之中,但是不排除未来某个时间会对其进行检查。

整体来看,虽然俄罗斯在立法上严格要求企业将数据本地化存储,并进行了积极的监督检查,但在执法处罚尺度上却相对温和。一方面,根据美国信息技术产业理事会介绍,俄方检查机构通常只检查书面文件(如与当地服务器服务商签订的合同),不检查服务商软硬件;另一方面,对于违反规定的企业,检查机构目前只是给予了轻微罚款和限制改正的处罚。

5 对我国实施跨境数据流动管理的启示

在数字经济时代,各国围绕数据资源的竞争空前激烈。我国无论是网络规模、用户规模,还是应用规模都是全球第一网络大国,而且随着“互联网+”的深入推进,大量的线下经济活动加速向线上迁移,网上数据总量保持指数增长态势,其蕴含的经济社会价值无可估量。借鉴俄方经验,要结合国情尽快确立我国跨境数据流动管理的基本规则,要敢于和善于执法,切实提升数据管理的执法效果。

5.1 加快推动跨境数据流动立法出台

俄罗斯通过数据立法活动为跨境数据流动管理提供了强有力的法理依据和执法保障。据跟踪了解,目前除俄罗斯以外,欧

⑧ <http://news.softpedia.com/news/Microsoft-Google-Adobe-Leave-Russia-Due-to-Putin-s-New-Laws-467521.shtml>

⑨ <http://www.bna.com/russias-2016-data-n57982066291/>

⑩ <http://www.hldataprotection.com/2016/02/articles/international-eu-privacy/russia-releases-data-localization-inspection-plan-for-2016/>

⑪ <http://www.hldataprotection.com/2016/06/articles/international-eu-privacy/russia-data-localization-update-results-from-regulatory-inspections-clarify-enforcement-approach/>

盟等都已通过立法手段强化数据跨境流动管理,力图将本国公民数据限制在境内存储。我国对某些特定行业和领域内的数据跨境流动做了限制性规定,例如《中华人民共和国保守国家秘密法》要求防止含有国家秘密的数据流出中国;《征信管理条例》规定信用机构必须在中国境内建立备份数据库,但仍缺乏对数据跨境流动管理的一般性规则。目前,我国在《中华人民共和国网络安全法》(二审稿)中要求“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的公民个人信息和重要业务数据应当在境内存储”。因数据跨境流动管理涉及多方利益诉求和责任分担,该条款也引发了较大的争议。建议在二审稿基础上对“关键信息基础设施”“个人信息”“业务数据”等概念做进一步明确界定,完善相关配套制度和措施,加快推动法案早日出台实施。

5.2 平衡数据留存本地化与产业发展关系

数据驱动的创新是当前培育新业态、改造提升传统产业的主要领域。充分发挥我国大数据产业体量大的优势,既要支持市场主体利用网络数据开展创新,还要把握好数据本地化存储的类型划分、成本负担、责任义务和例外条款。俄罗斯虽然严格规定了数据本地存储的要求,但也规定了同等保护的例外情况,并且选择了较为温和的执法方式,没有完全挤压企业生存

和发展的空间。当前我国大数据产业发展呈现上升之势,基于大数据的创业创新不断涌现,国内企业对数据流动也存在一定需求。建议我国在立法中对数据跨境进行分类管理,凡是涉及国家秘密、社会安全以及经济安全的数据,必须在境内的数据中心存储和处理;对普通的个人数据,允许其通过合同监管等方式,在满足双方约定条件前提下允许其跨境流动,在保护安全的同时为产业发展留下一定的空间。

5.3 提升跨境数据流动管理执法水平

俄罗斯监管部门以立法为依据,配备专门工作人员,制定年度详细的检查计划,积极开展执法监督检查活动,企业普遍守法,取得了不错的效果。制度的生命力在于实施,在明确立法规则的同时,要强化执法监督检查,督导企业更好地履行义务,规范网络数据管理行为。2015年中央新“三定”方案授权了电信主管部门电信网、互联网网络数据管理职责^①,但目前我国实践监管中仍以行业监管为主,而数据跨境流动监管具有较强的技术性、专业性,不同行业间的执法水平和执法手段差异明显。建议尽快明确跨境数据管理体制,或设立专门的数据执法监管机构或借鉴俄方经验配备专门工作人员,完善监管手段,建立企业数据保护信用记录,采取不定期抽查等方式,提升数据跨境流动管理的执法水平。

①

<http://www.miit.gov.cn/n1146285/c3722500/content.html>

作者简介



何波(1989-),男,就职于中国信息通信研究院互联网法律研究中心,罗马国际统一私法协会研究访问学者,曾获工业和信息化部首届青年干部论文大赛一等奖,主要从事信息通信、互联网等相关法律政策以及国际贸易规则相关方面的研究,参与我国《电子商务法》《网络安全法》《关于加快构建大众创业万众创新支撑平台的指导意见》等立法和政策的起草支撑及研究工作。

收稿日期:2016-09-08